AMENDMENTS TO THE CLAIMS

Please amend the claims of the present application as set forth below. In accordance with the PTO's revised amendment format, a detailed listing of all claims is provided. A status identifier is provided for each claim in a parenthetical expression following each claim number. Changes to the claims are shown by strikethrough (for deleted matter) or underlining (for added matter).

Claims 3, 4, 6-12, 15-22 and 25-30 were pending at the time of the Office Action.

Claims 3, 4, 6-12, 15-22 and 25 are expressly allowed.

Claims 26 and 28-30 are rejected.

Claim 27 is objected to.

Claims 27-30 are amended by the current response.

Claim 26 is canceled by the current response.

Accordingly, claims 3, 4, 6-12, 15-22, 25 and 27-30 remain pending.

1. (Previously Canceled)

2. (Previously Canceled)

3. (Previously Amended) A computerized method for key-based secure storage comprising:

downloading information and an access predicate that specifies requirements for an application to access the information;

generating a seed value;

producing a hash seed value based on the seed value using a one-way hash function;

generating an application storage key from the hash seed value;

encrypting the information using the application storage key; and

associating the access predicate with the encrypted information.

14. (Previously Amended) A computerized method for key-based secure storage comprising:

downloading information and an access predicate that specifies requirements for an application to access the information;

generating a seed value;

producing a first hash seed value based on the seed value using a one-way hash function;

producing a second hash seed value based on the seed value and a user identifier using a keyed hash function;

generating a user storage key from the second hash seed value;

encrypting the information using the user storage key; and

associating the access predicate with the encrypted information.

5. (Previously Canceled)

16. (Previously Amended) A computerized method for key-based secure storage comprising:

downloading information and an access predicate that specifies requirements for an application to access the information;

obtaining a storage key;

encrypting the information using the storage key;

associating the access predicate with the encrypted information;

obtaining an operating system storage key;

encrypting the access predicate with the operating system storage key; and

encrypting a plurality of other storage keys using the operating system storage key, wherein the other storage keys are selected from the group consisting of application storage keys and user storage keys.

17. (Previously Amended) A computerized method for key-based secure storage comprising:

downloading information and an access predicate that specifies requirements for an application to access the information;

obtaining a storage key;

encrypting the information using the storage key;

associating the access predicate with the encrypted information;

generating a seed value;

generating an operating system storage key based on the seed value; and

encrypting the access predicate with the operating system storage key.

18. (Previously Amended) A computerized method for key-based secure storage comprising:

downloading information and an access predicate that specifies requirements for an application to access the information;

generating a seed value for the application;

producing an application hash seed value based on the seed value for the application using an application-specific one-way hash function;

generating an application storage key from the application hash seed value;

generating a seed value for a user;

producing a first user hash seed value based on the seed value for the user using a one-way hash function;

producing a second user hash seed value based on the first user hash seed value and a user identifier using a keyed hash function;

generating a user storage key from the second user hash seed value, the application storage key and the user storage key to encrypt information containing a portion specific to an application and a portion specific to the user;

encrypting the information using the application storage key and the user storage key; and

associating the access predicate with the encrypted information.

19. (Previously Amended) A computerized method for key-based secure storage comprising:

downloading information and an access predicate that specifies requirements for an application to access the information;

obtaining a storage key;

encrypting the information using the storage key;

associating the access predicate with the encrypted information;

storing the storage key in a key vault provided by a third-party; and

recovering the storage key from the key vault.

10. (Original) The computerized method of claim 6, wherein recovering the storage key comprises:

requesting recovery of the storage key; and

providing information to the third-party to enable validation of the request.

11. (Previously Amended) The computerized method of claim 6, further comprising:

selecting the key vault from a plurality of key vaults provided by a trusted operating system.

12. (Previously Amended) The computerized method of claim 6, further comprising:

selecting the key vault designated by a provider of the information.

13. (Previously Canceled)

14. (Previously Canceled)

15. (Previously Amended) A computer system comprising:

a processing unit;

a system memory coupled to the processing unit through a system bus;

a computer-readable medium coupled to the processing unit through a system bus;

a generate key function executed from the computer-readable medium by the processing unit, wherein the generate key function causes the processing unit

to generate an operating system storage key based on an identity for the operating system and based on a seed.

16. (Previously Amended) A computer system comprising:

a processing unit;

a system memory coupled to the processing unit through a system bus;

a computer-readable medium coupled to the processing unit through a system bus;

a generate key function executed from the computer-readable medium by the processing unit, wherein the generate key function causes the processing unit to generate an operating system storage key based on an identity for the operating system;

an application specific one-way hash function executed from the computer-readable medium by the processing unit, wherein the application specific one-way hash function causes the processing unit to generate an application storage key from a hashed seed; and

a generate application key function executed from the computer-readable medium by the processing unit, wherein the generate application key function causes the processing unit to generate the hashed seed from an application seed.

17. (Previously Amended) A computer system comprising:

a processing unit;

a system memory coupled to the processing unit through a system bus;

a computer-readable medium coupled to the processing unit through a system bus;

a generate key function executed from the computer-readable medium by the processing unit, wherein the generate key function causes the processing unit to generate an operating system storage key based on an identity for the operating system;

a key-hash function executed from the computer-readable medium by the processing unit, wherein the key-hash function causes the processing unit to generate a user storage key from a hashed seed and an identity for the user;

a one-way hash function executed from the computer-readable medium by the processing unit, wherein the one-way hash function causes the processing unit to generate the hashed seed from a previously hashed seed; and

a generate user key function executed from the computer-readable medium by the processing unit, wherein the generate user key function causes the processing unit to generate the previously hashed seed from a user seed.

18. (Previously Amended) A computer system comprising:

a processing unit;

a system memory coupled to the processing unit through a system bus;

a computer-readable medium coupled to the processing unit through a system bus; and

a trusted operating system executed from the computer-readable medium by the processing unit, wherein the trusted operating system causes the processing unit to encrypt downloaded information using a storage key based on a seed value.

19. (Previously Amended) The computer system of claim 18, wherein the trusted operating system further causes the processing unit to encrypt an access predicate associated with the downloaded information using an operating system storage key, to encrypt the seed value for the storage key using the operating system storage key, and to associate the encrypted access predicate with the encrypted seed value.

20. (Previously Amended) The computer system of claim 19, wherein the trusted operating system further causes the processing unit to validate each application requesting access to the downloaded information using the access predicate, and decrypts the seed value for use by a validated application.

21. (Previously Amended) The computer system of claim 18, wherein the storage key used to encrypt the downloaded information is specific to an application.

22. (Previously Amended) The computer system of claim 18, wherein the storage key used to encrypt the downloaded information is specific to a user.

23. (Previously Canceled)

24. (Previously Canceled)

25. (Previously Added) A computerized method for key-based secure storage comprising:

downloading information and an access predicate that specifies requirements for an application to access the information;

obtaining a storage key;

encrypting the information using the storage key;

associating the access predicate with the encrypted information;

storing the storage key in a key vault provided by a third-party;

recovering the storage key from the key vault; and

selecting the key vault from a plurality of key vaults provided by an authenticated operating system.

26. (Currently Canceled)

27. (Currently Amended) A computer system comprising;

a processing unit;

a system memory coupled to the processing unit through a system bus;

a computer-readable medium coupled to the processing unit through a system bus; and

an authenticated operating system configured to execute on the processing unit from the computer-readable medium, the authenticated operating system causing the processing unit to encrypt downloaded information using a storage key based on a seed value;

~~The computer system of claim 26,~~ wherein the authenticated operating system further causes the processing unit to encrypt an access predicate associated

with the downloaded information using an operating system storage key, to encrypt the seed value for the storage key using the operating system storage key, and to associate the encrypted access predicate with the encrypted seed value.

20 19

~~28~~. (Currently Amended) The computer system of claim ~~26~~ ~~27~~, wherein the authenticated operating system further causes the processing unit to validate each application requesting access to the downloaded information using the access predicate, and decrypts the seed value for use by a validated application.

21 19

~~29~~. (Currently Amended) The computer system of claim ~~26~~ ~~27~~, wherein the storage key used to encrypt the downloaded information is specific to an application.

22 19

~~30~~. (Currently Amended) The computer system of claim ~~26~~ ~~27~~, wherein the storage key used to encrypt the downloaded information is specific to a user.